Warszawa, 14.08.2024 r.

Sygnalista zgłasza naruszenie RODO – czyli dlaczego privacy by design jest tak ważne podczas tworzenia procedury dotyczącej zgłoszeń wewnętrznych.

Nieco ponad miesiąc dzieli nas od zakończenia vacatio legis Ustawy o ochronie sygnalistów z dnia 14 czerwca 2024 r.

W poprzednich naszych publikacjach zwracaliśmy uwagę na obowiązki w kontekście zapewnienia zgodności z RODO w związku z wdrożeniem wymogów Ustawy o ochronie sygnalistów. [1]

Z perspektywy najważniejszych obowiązków, na czas wymagalności wdrożenia procedury przyjmowania i rozpatrywania zgłoszeń wewnętrznych będą oczywiście:

a. przygotowanie klauzul informacyjnych dla sygnalisty, dla świadka, dla osoby, której dotyczy zgłoszenie (tu tylko jeśli nie zachodzą przesłanki wyłączające konieczność realizacji obowiązku informacyjnego);
b. aktualizacja rejestru czynności przetwarzania – o nowe czynności objęte procedurą, a także w przypadku powierzenia procesu przyjmowania zgłoszeń zewnętrznemu podmiotowi – o kwestie podwykonawców tego przetwarzania i stosowane zabezpieczenia przetwarzanych danych;
c. przeprowadzenie oceny skutków przetwarzania danych osobowych dla tych operacji, ponieważ zgodnie z komunikatem UODO, w zakresie korzystania z systemów whistleblowing taka ocena jest konieczna. Nie zaszkodzi jednak interpretować realizacji tego wymogu wprost z art. 35 ust. 1 RODO, zgodnie z którym: „jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych". Zatem nową technologię możemy rozpatrywać również w kontekście nowego procesu/nowych narzędzi wykorzystywanych w procesie, który może powodować wysokie ryzyko naruszenia praw lub wolności, a nie tylko w kontekście innowacyjnego charakteru wdrażanej technologii;
d. przygotowanie upoważnień do przetwarzania danych osobowych w związku z pełnieniem obowiązków związanych z przyjmowaniem i/lub prowadzeniem działań następczych;
e. aktualizację polityk retencji w zakresie danych osobowych, które administrator może ocenić jako niemające znaczenia w rozpatrywanej sprawie, danych osobowych przetwarzanych w rejestrze zgłoszeń oraz dokumentacji pochodzącej z działań następczych.

Powyższa checklista nie podejmuje jednak problematyki związanej z trybem postępowania, jaki należy przewidzieć w sytuacji, gdy zgłoszenie naruszenia prawa będzie dotyczyło gałęzi ulubionej przez każdego Inspektora Ochrony Danych (IOD).

Chodzi oczywiście o zgłoszenie naruszenia prawa w zakresie ochrony prywatności i danych osobowych. Ta gałąź przepisów została wprost wskazana w art. 3 ust. 1 pkt 13 Ustawy.

Zgłoszenie to, zgodnie z przyjętą procedurą, może zostać dokonane z zachowaniem poufności tożsamości sygnalisty, jak i anonimowo (jeśli podmiot prawny zdecydował się na taką możliwość).

Pojawia się więc pytanie: co w sytuacji, kiedy zgłoszenie zostanie dokonane anonimowo, wymaga doprecyzowania, czyli podjęcia kontaktu z sygnalistą, np. „pracownicy działu handlowego kopiują dane osobowe z bazy CRM i sprzedają konkurencji wraz z informacjami o zadłużeniu naszych klientów"? Pojawi się praktyczne pytanie – od kiedy zaczyna biec magiczny czas 72h na ewentualne zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych?

Moment stwierdzenia naruszenia następuje w przypadku, gdy administrator ma wystarczający stopień pewności co do tego, że doszło do zdarzenia zagrażającego bezpieczeństwu, które doprowadziło w konsekwencji do naruszenia bezpieczeństwa danych osobowych. Zatem aby tę pewność uzyskać, natychmiast po powzięciu takiej informacji powinny zostać wszczęte działania następcze polegające na ustaleniu, czy do takiego naruszenia faktycznie może dochodzić. W zakresie rozliczalności należy zapewnić udokumentowanie tych działań (np. wyniki z systemu DLP weryfikującego działania na kontach handlowców, np. w zakresie zgrywania danych z CRM na prywatne zasoby (pendrive, chmura) lub protokół z przesłuchania pracowników działu handlowego). Moment stwierdzenia naruszenia powinien być więc liczony od momentu powzięcia wystarczającej pewności w zakresie tego, czy doszło do incydentu prowadzącego do naruszenia ochrony danych osobowych czy też nie.

Nie należy natomiast w działaniach następczych upatrywać furtki do maksymalnego wydłużania czasu, jaki wynika z art. 33 ust. 1 RODO.

Zatem w przypadku zgłoszeń dotyczących naruszeń przepisów w zakresie ochrony danych osobowych ważne będzie zwracanie uwagi na jak najszybsze podjęcie działań następczych celem określenia nie tylko samych skutków zdarzenia, ale też momentu stwierdzenia naruszenia.

Drugim praktycznym problemem, jaki może pojawić się w związku z dodatkowym kanałem zgłaszania naruszeń, jest włączanie IOD w skład komórki odpowiedzialnej za prowadzenie działań następczych.

Zarówno nasza krajowa ustawa, jak i dyrektywa unijna nie zakazują wprost takiego rozwiązania. Jednak zgodnie ze stanowiskiem UODO: „W takiej sytuacji administrator przed powierzeniem osobie pełniącej funkcję IOD innych zadań lub obowiązków (w tym przypadku polegających na przyjmowaniu zgłoszeń sygnalistów oraz prowadzeniu postępowań wyjaśniających) powinien dokonać starannej analizy w zakresie zapewnienia IOD właściwych warunków dla zachowania jego niezależności i prawidłowego wykonywania zadań. Ocena ta powinna być dokonana przy uwzględnieniu stosownych przepisów RODO oraz Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243).

Zgodnie bowiem z art. 38 ust. 6 RODO IOD może wykonywać „inne zadania i obowiązki". W dalszej części przepisu występuje jednak zastrzeżenie, iż „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów". [2] Zatem zarówno, jeśli dla dobra prowadzonego postępowania wyjaśniającego – włączenie IOD do zespołu odpowiedzialnego za działania następcze będzie miało charakter jednorazowy, jak i w sytuacjach, kiedy IOD będzie członkiem tego zespołu na stałe – wymagana jest rozliczalność w zakresie wykazania niezależności i braku konfliktu interesu w związku z łącznym pełnieniem dwóch funkcji w organizacji.

Jeszcze innym praktycznym problemem do podjęcia będzie sytuacja, kiedy zgłoszenie dotyczące naruszenia będzie złożone w sposób zapewniający ochronę tożsamości sygnalisty, a dojdzie do jej przypadkowego lub celowego ujawnienia w toku przyjęcia zgłoszenia bądź prowadzenia działań następczych.

Pojawi się swoisty RODO krindż – polegający na wystąpieniu naruszenia podczas obsługi naruszenia. Ujawnienie tożsamości sygnalisty może stanowić wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą, ze względu na potencjalne negatywne konsekwencje dla sygnalisty, takie jak działania odwetowe. Zgodnie z art. 33 RODO, administrator danych jest zobowiązany do zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, jeżeli naruszenie to może powodować ryzyko naruszenia praw lub wolności osób fizycznych.

W kontekście ochrony sygnalistów, ujawnienie tożsamości sygnalisty należy uznać za poważne naruszenie, które co do zasady powinno być zgłoszone do Prezesa UODO. Jest to uzasadnione szczególną ochroną przyznaną sygnalistom przez ustawę oraz potencjalnymi poważnymi konsekwencjami ujawnienia ich tożsamości.

Tu szczególnie przyda się rewizja procedury postępowania z incydentami/naruszeniami w kontekście jej współgrania z procedurą zgłoszeń wewnętrznych. Jeśli procedura zgłaszania naruszeń zakłada powiadamianie IOD poprzez np. zgłoszenie naruszenia na konkretną skrzynkę email, a IOD nie znajduje się w kręgu osób upoważnionych do przetwarzania danych w ramach przyjmowania zgłoszeń i prowadzenia działań następczych zgodnie z wymogami ustawy o ochronie sygnalistów, to... przerzucając bezwiednie do IOD treść zgłoszenia złożonego w formie e-mail, możemy ujawnić tożsamość sygnalisty osobie nieupoważnionej.

Napisanie procedury zgłoszeń wewnętrznych to nie wszystko. W ramach zasady privacy by design – procedura powinna być stworzona w taki sposób, aby zespół odpowiedzialny za jej przygotowanie, na etapie prac nad tekstem zapewniał poszanowania zasad ochrony danych osobowych na każdym etapie procesu oraz przeanalizował możliwe przypadki zgłoszeń i sposób obiegu i przechowywania danych w związku z prowadzonymi działaniami następczymi.

Generowanie naruszeń podczas obsługi naruszeń – to porażka systemu ochrony danych osobowych. Nie bójmy się włączać IOD w prace nad procedurą.

[1] https://www.isecure.pl/blog/ustawa-o-sygnalistach-w-koncu-uchwalona-nowe-wyzwania-pod-katem-ochrony-danych-osobowych/
[2] https://uodo.gov.pl/pl/495/2415

Magdalena Jacolik

Specjalista ds. ochrony danych osobowych